In the United States Court of Federal Claims

SALIENSE CONSULTING LLC,

Plaintiff,

v.

THE UNITED STATES,

Defendant,

and

DELVIOM LLC,

Defendant-Intervenor.

No. 25-624
(Filed: June 23, 2025)[1]

John Edward McCarthy, Jr., Zachary H. Schroeder, and Issac D. Schabes, Crowell & Moring LLP, Washington, D.C., for Plaintiff.

Nelson Kuan, Civil Division, United States Department of Justice, Washington, D.C., and *Robert B. Nelson*, United States Department of Homeland Security, Washington, D.C., for Defendant.

Elizabeth N. Jochum, Samarth Barot, Shane Hannon, and Amanda DeLaPerriere, Blank Rome, LLP, Washington, D.C., for Defendant-Intervenor.

OPINION AND ORDER

LERNER, *Judge*.

Plaintiff, Saliense Consulting LLC ("Saliense"), brings this bid protest against the United States. Am. Compl., ECF No. 23. Defendant awarded a contract for cybersecurity services to Defendant-Intervenor, Delviom LLC ("Delviom"). Saliense challenges Defendant's determination that an individual Plaintiff proposed for a key role in the procurement was not sufficiently experienced in one of the required qualifications, continuous monitoring. This decision rendered Saliense ineligible to receive the award.

Pending before this Court are the parties' respective Motions for Judgment on the Administrative Record, as well as Defendant-Intervenor's Partial Motion to Dismiss Under Rule

[1] This Opinion was filed under seal on June 12, 2025. ECF No. 35. The parties were afforded fourteen days to propose redactions. *Id.* Plaintiff proposed redactions, and Defendant and Defendant-Intervenor do not oppose. ECF No. 37. Accordingly, the Court reissues this Opinion with the agreed upon redactions, which are noted with bracketed asterisks ([***]).

12(b)(6). Pl.'s Mot. for J. on the Admin. R. (hereinafter "Pl.'s Mot."), ECF No. 25; Def.'s Cross-Mot. for J. on the Admin. R. (hereinafter "Def.'s Mot."), ECF No. 24; Def.-Intervenor's Mot. for J. on the Admin. R. and Partial Mot. to Dismiss Under Rule 12(b)(6) (hereinafter "Def.-Intervenor's Mot."), ECF No. 26. For the reasons below, Plaintiff's Motion for Judgment on the Administrative Record is **DENIED**. Defendant-Intervenor's Partial Motion to Dismiss is **GRANTED**, and its and Defendant's Motions for Judgment on the Administrative Record are **GRANTED**.

I. Factual Findings

A. The Solicitation

In August 2024, the Department of Homeland Security ("DHS" or "the Agency") issued a Request for Quote ("RFQ" or "Solicitation") for cybersecurity services as a set-aside for small businesses. Tab 15a at AR 719–20. *See* Tab 66 at AR 2253. The awardee was to provide cybersecurity support services to the National Security Cyber Division and the Enterprise Cybersecurity Governance Division within DHS' Chief Information Security Officer Directorate ("CISOD"). Tab 15a at AR 739. The Federal Acquisition Regulation ("FAR") 8.405 and DHS acquisition guidelines governed the procurement. *Id.* at AR 720. The Agency would choose the quote representing "the best overall value to the Government, considering the technical evaluation factors and price." *Id.*

B. Evaluation Criteria

The Agency conducted this procurement in three phases. *Id.* at AR 722. Quoters submitted separate submissions called volumes for each phase. *Id.* The following Table illustrates the submission process:

Phase	Volumes/Selections
Phase 1 **Mandatory Down-Select**	Factor 1: Facility Clearance
Phase 2 **Advisory Down-Select**	Factor 2: Prior Corporate Experience
Phase 3	Factor 3: Management & Staffing Approach
	Factor 4: Technical Qualifications & Approach
	Factor 5: Cybersecurity Readiness
	Factor 6: Price

Id. at AR 723–24.

Under the first phase, quoters submitted evidence they held active Facility Clearance at the Top-Secret level. *Id.* at AR 723, 725. The DHS required all offerors to maintain Top-Secret level Facility Clearance to be eligible for the contract. *Id.* at AR 725, 734.

Offerors who proceeded to Phase 2 provided the Agency with information about their Prior Corporate Experience. *Id.* at AR 723, 726. After reviewing these submissions, DHS advised the highest-rated quoters to proceed with the submission process. *Id.* at AR 726–27. Defendant informed all other quoters they were "unlikely to be viable competitors" and provided a basis for its "advisory recommendation." *Id.* Still, quoters who were advised not to proceed to Phase 3 of the procurement could continue participating in the bidding process. *Id.* at AR 727.

Under Phase 3, the Agency reviewed four more factors: Management & Staffing Approach, Technical Qualifications & Approach, Cybersecurity Readiness, and Price. *Id.* at AR 727–33.

For Management & Staffing Approach, the Agency instructed offerors to "provide sufficient information to demonstrate a definitive and comprehensive approach to managing and staffing, so that the Government can determine its level of confidence in the Offeror's understanding of the requirements, ability to perform against the Task Order, and the likelihood of successful Task Order performance." *Id.* at AR 727.

Quoters provided a list of key personnel and then "demonstrate[d] that the proposed key personnel [met] the minimum qualifications listed in the Key Personnel section of the Statement of Work [("SOW")] (section 4.3)." *Id.* at AR 728. Key personnel were "those Contractor personnel considered to be essential to the performance of this requirement." *Id.* at AR 778. Submissions needed to "include resumes for the proposed key personnel to fill the positions identified in SOW section 4.3. The resumes [had to] contain, at a minimum[:] company name and address, telephone number, point of contact, overview of duties and the dates employed." *Id.*

To emphasize the importance of this condition, Defendant wrote in the Solicitation: "Note: Resumes must clearly demonstrate the proposed personnel meet the key personnel minimum qualifications." *Id.* Proposals were judged based on the clarity and feasibility of the roles, the responsibilities of the quoter's team, how their management approach described day-to-day operations, and whether the quotation demonstrated the offeror's ability to recruit, hire, train, and retain qualified staff. *Id.* at AR 735.

The Agency identified six positions as essential to contract performance—one of which was the Cybersecurity Reporting Lead. *Id.* at AR 778–79. A proposed Cybersecurity Reporting Lead needed "10 years of experience in cybersecurity, including at least four years of specialized experience involving continuous monitoring." *Id.* at AR 779. The Cybersecurity Reporting Lead would have "high-level responsibility" for the following functions:

- CISOD Governance, Risk, and Compliance Program Tool Development and Support
- Cybersecurity Metrics and Reporting
- Cybersecurity Risk Analysis and [Federal Information Security Management Act ("FISMA")] Reporting
- Continuous Monitoring
- Risk Management and Quantification

- Plan of Action & Milestones (POA&M) Reporting

Id. at AR 781 (Section 4.3.3 Cybersecurity Reporting Lead).

Further, the Cybersecurity Reporting Lead would be responsible for all contractor work performed under Section 2.8 of the Solicitation and would handle various cybersecurity risk analysis tasks under the contract. *Id.* *See also id.* at AR 763–70 (listing the various duties of the Cybersecurity Reporting Lead under Task Area Eight), 777. Section 2.8.4 of the Solicitation described the position's responsibilities pertaining to continuous monitoring:

> 2.8.4 Continuous Monitoring
>
> **The Contractor shall:**
>
> a. Provide research and development support of data analytic and data management technologies including those associated with collecting, analyzing, parsing, and reporting large volumes of data.
>
> b. Provide installation and technical support for DHS CISOD and DHS components regarding issues, data feed submissions, and interfaces to the DHS FISMA Compliance Tool suite.
>
> c. Work with federal lead, develop suggestions for guidance and policy regarding virtual environments affecting Continuous Monitoring[.]
>
> d. Develop procedures for the continuous monitoring of devices assessing DHS networks that are outside the scope of current manual and automated capabilities to ensure visibility of all systems. These devices may include smart phones, tablets, and other emerging mobile devices.
>
> e. Engage with and support working group and internal project team meetings with DHS Components. Document DHS Component feedback and provide recommendations as needed.
>
> f. Support current and future enhancements and transition of DHS CISOD tools and requirements. Continuous Monitoring [point of contact] should be able to generate scripts, queries primarily in MS SQL Splunk, and Elastic.

Id. at AR 767–68.

The Solicitation's text did not contain a definition of continuous monitoring. *See* Tab 15a. However, it directed offerors to a non-exhaustive list of mandatory documents with which an awardee needed to comply to meet performance requirements. *Id.* at AR 742–43, 739 (elaborating on the performance requirements). One of those documents, the DHS Information Systems Continuous Monitoring Strategy, explained in its introduction: "Information Security Continuous Monitoring (ISCM) is essential in allowing the Department of Homeland Security (DHS) to leverage operational efficiency and defend against evolving threats." Tab 12f at AR 259. It established "[t]he National Institute of Standards and Technology (NIST) Special Publications (SP) 800-137, 'Information Security Continuous Monitoring for Federal

Information Systems and Organizations,' defines ISCM as 'maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.'" *Id.* (quoting Tab 12h at AR 453, 455, 498). The guidance also clarifies the process for developing an ISCM strategy under NIST SP 800-137, as well as other NIST guidance like NIST 800-37 and NIST Risk Management Framework ("RMF") Step 6. *Id.* *See also* Tab 12h at AR 463–64 (explaining the relationship among these documents).

NIST SP 800-137 does not appear in the list of mandatory compliance documents in the RFQ. *See* Tab 15a at AR 742–43. But it does appear, along with other instruments discussing continuous monitoring, in a list of documents that "may be helpful to the Contractor in performing the tasks described" in the Solicitation. *Id.* at AR 743. *See also* Tab 12g (explaining how the Risk Management Framework for information systems and organizations provides a process for managing security and privacy risks related to continuous monitoring).

C. Saliense's Proposed Cybersecurity Reporting Lead

Having been advised it was among the highest rated offerors in Phase 2, Saliense submitted its Phase 3 quote on September 11, 2024. *See, e.g.*, Tab 29b; Tab 33a at AR 1072 (Volume III – Management, Technical, Cybersecurity Readiness). It proposed [***] [***] as its Cybersecurity Reporting Lead and provided her resume. *Id.* at AR 1085–86. At the time of submission, Ms. [***] served as Saliense's Senior Cybersecurity "SME"; a job she began in November 2023. *Id.* at AR 1085. However, Ms. [***] only listed her job title without any description of her role or responsibilities. *See id.* This facially violated the Solicitation's requirements. *See* Tab 15a at AR 728 (requiring resumes contain an "overview of duties" and "clearly demonstrate the proposed personnel meet the key personnel minimum qualifications").

According to her resume, from May 2020 to November 2023, Ms. [***] worked as a Senior Security Controls Assessor for Business Integra Remote. Tab 33a at AR 1085. The resume states she "[c]onducted and developed associated reporting for security control assessments to assess the adequacy of management, operation, privacy, and technical security controls implemented"; "[r]eviewed and analyzed results from vulnerability scanning tools such as Nessus, WebInspect, etc."; and "[c]onducted systems risk assessment through risk analysis, assess [sic] assets within systems boundaries, and identify [sic] all possible vulnerabilities within systems." *Id.*

Further, she worked as a Senior Cybersecurity Analyst at Zeneth Technology Partners from August 2017 to April 2020. *Id.* There she "[c]onducted I.T. controls risk assessment that includes [sic] reviewing organizational policies, standards and procedures and provide [sic] advice on their adequacy, accuracy and compliance with FISMA and [the Federal Risk and Authorization Management Program ("FEDRAMP")]" and "[s]upported the FISMA compliance program by reviewing evidence of compliance, driving necessary system and process improvements, and ensure [sic] the completion of the annual compliance reports." *Id.* She also was "[r]esponsible for the development of [a] security control test plan and in-depth security assessment of information systems to maintain FISMA and FEDRAMP compliance by

implementing guidelines and standards identified in the National Institute of Standard and Technology (NIST) 800-53A." *Id.*

D. Litigation History

Twelve bidders submitted Phase 3 quotes, and DHS did not award the contract to Saliense. Tab 43a at AR 1509. Saliense received a low confidence score under the Management & Staffing Approach factor. Tab 45 at AR 1526. DHS found Saliense's proposed Cybersecurity Reporting Lead, Ms. [***], did not have at least four years of specialized experience involving continuous monitoring. *Id*. at AR 1530, 1532 ("Saliense Consulting, LLC's proposed Cybersecurity Reporting Lead has no apparent experience in continuous monitoring."). The Agency explained there was a deficiency related to Ms. [***]'s resume, observing "there is no evidence in the resume that this individual has served in a capacity where their professional responsibilities would have included active monitoring of systems to ensure continued compliance with cybersecurity requirements in operations." *Id.* at AR 1530.

Saliense protested the Agency's decision at the U.S. Government Accountability Office ("GAO") on October 10, 2024. *See generally* Tab 50. DHS proposed reexamination of Ms. [***]'s resume, and on November 12, 2024, GAO dismissed the protest because the Agency planned to take corrective action. Tab 51; Tab 52.

E. Saliense's Reevaluation

After reconsidering Ms. [***]'s resume during its corrective action, Defendant again determined it had "low confidence that [Saliense] understands the requirement, provides sufficient information, or will be successful in performing the task order requirements." Tab 76 at AR 2411. The Agency found Ms. [***]'s resume failed to meet the contract requirements because she did not have "at least four years of specialized experience involving continuous monitoring." *Id.* at AR 2413 (emphasis omitted). Her resume demonstrated "extensive experience conducting security control assessments" and "risk management activities," as well as in "guiding system owners through the authority to operate (ATO process)." *Id.* However, the resume did not show she had ever "served in a capacity where [her] professional responsibilities would have included active monitoring of systems to ensure continued compliance with cybersecurity requirements in operations." *Id.* "As such, the resume [did] not show the individual possesses the required at least four years of specialized experience involving continuous monitoring." *Id.*

Defendant opined—as it did in its original evaluation of Saliense—that in her present job, Ms. [***] could possibly engage in continuous monitoring activities even though "no actual description of [her] current role is included in the resume—only a job title of 'Senior Cybersecurity SME' is listed." *Compare id.* at AR 2413 *with* Tab 43a. But even if she performed continuous monitoring practices in her current role, she had worked less than a year in this position when Saliense submitted its proposal—far shy of the four-year minimum requirement for continuous monitoring experience in the Solicitation. Tab 76 at AR 2413. And Saliense provided no description of her activities in this job. Tab 33a at AR 1085.

Further, DHS found Ms. [***]'s description of her work as a Senior Security Controls Assessor at Business Integra Remote insufficient to establish she had sustained experience in continuous monitoring. *Id.* at AR 2415–16. While her resume described reviewing and analyzing results from vulnerability scanning tools,

> these activities are more focused on single one time [sic] post-assessment actions rather than continuous monitoring which need [sic] to include development, implementation and execution of methodologies and tools to automate and continuously assess risk and make decisions, and there is no mention of development, implementation or execution of real-time or near-real-time monitoring of security events, incidents, or system status over time.

Id. at AR 2416.

Drawing on the definition from NIST SP 800-137, DHS explained:

> [c]ontinuous monitoring differs from the listed responsibilities in the resume, in that continuous monitoring is operational in nature, involving the use of different tools and techniques than the analysis of a system that is not yet operating, to perform the active monitoring of systems after they have been authorized to operate, to ensure continued acceptable cybersecurity risk posture.

Id. at AR 2413. *See also* Tab 12h at AR 496 (defining "continuous monitoring" as "maintaining ongoing awareness to support organizational risk decisions"); *id.* at AR 453, 455, 498 (defining ISCM). In Defendant's view:

> [a] person who has never performed these duties, even if they are very familiar with governance, risk management, and compliance (as this person seems to be) would not be able to advise or assist the government in execution and ongoing improvement of the existing DHS continuous monitoring program, which is required under the SOW, and essential for mission success.

Tab 76 at AR 2413.

The Agency concludes "the candidate's resume does not cover most of the specified responsibilities" listed under Section 2.8.4, "especially those related to tools, continuous monitoring of mobile and emerging devices, supporting working groups, developing procedures and policies, and using specific technologies." *Id.* at AR 2419. Ms. [***] had strong experience in cybersecurity assessments and FISMA compliance, but she "lack[ed] direct involvement in the more technical and developmental tasks, especially those related to continuous monitoring and tool development." *Id.* "Overall, the recommended candidate's resume does not fully cover all the required activities stated by the RFQ in section 4.3.3 for the Cybersecurity Reporting Lead role." *Id.*

In a memorandum to Contracting Officer Kierra Buggs, Donald E. Yeske, the Task Order Designated Selection Official, expounded on why DHS continued to believe Saliense correctly received a deficiency for the Cybersecurity Reporting Lead position. *See generally* Tab 77 (Memorandum re Corrective Action and Reconsideration of the Award Decision). In two paragraphs, Mr. Yeske explained the procurement's Technical Evaluation Team concluded that

Ms. [***]'s resume did not demonstrate any experience in continuous monitoring. *Id.* at AR 2425. Because of this, the Team deemed Saliense's quote ineligible for the award. *Id.* Mr. Yeske incorrectly referred to the Cybersecurity Reporting Lead as the "Continuous Monitoring Lead" twice. *Id.*

On March 26, 2025, DHS notified Plaintiff of its decision after completing its reevaluation of Ms. [***]'s resume. Tab 78.2 at 2435. Defendant again concluded her resume did not demonstrate any experience in Continuous Monitoring. *Id.* The Agency "require[d] four (4) years of specialized experience *in* Continuous Monitoring for this key position," and "[t]he resume demonstrated no specialized NIST RMF Step 6 experience." Tab 78.2 at AR 2435 (emphasis added). *See also* Am. Compl. at 17. This deficiency made Saliense ineligible for the award. *Id.* Saliense objected to this finding at GAO, but its protest was dismissed. *See generally* Tab 81.

II. Procedural History

On April 10, 2025, Saliense filed a Complaint in this Court challenging its elimination from the procurement. Compl., ECF No. 1. The Court granted Delviom's request to intervene on April 17, 2025. Defendant provided the Administrative Record for this case on April 18, 2025. *See* ECF No. 22. Plaintiff filed an Amended Complaint on April 25, 2025. Am. Compl. On May 2, 2025, the parties filed their Motions for Judgment on the Administrative Record, and Defendant-Intervenor filed its Partial Motion to Dismiss Under Rule 12(b)(6). Def.'s Mot.; Pl's Mot.; Def.-Intervenor's Mot. Six days later, the Court granted Defendant's unopposed Motion to Complete the Administrative Record. *See* ECF No. 27. The next day, the parties filed their Responses, and on May 16, 2025, they filed their Replies. Def.'s Resp. to Pl.'s Mot. for Judgment on Admin. R. (hereinafter "Def.'s Resp."), ECF No. 28; Pl.'s Resp. to Def.'s & Def.'s-Intervenor's Mots. for J. on the Admin. R. & Def.'s-Intervenor's Partial Mot. to Dismiss (hereinafter "Pl.'s Resp."), ECF No. 29; Def.-Intervenor's Resp. to Pl.'s Mot. for J. on the Admin. R. (hereinafter "Def.-Intervenor's Resp."), ECF No. 30; Def.'s Reply, ECF No. 31; Pl.'s Reply, ECF No. 32; Def.-Intervenor's Reply, ECF No. 33.

III. Jurisdiction and Standard of Review

The U.S. Court of Federal Claims has jurisdiction over protests by "an interested party objecting to a solicitation by a Federal agency for bids or proposals for a proposed contract . . . or any alleged violation of statute or regulation in connection with a procurement or a proposed procurement." 28 U.S.C. § 1491(b)(1). A plaintiff challenging a procurement decision must demonstrate they have both Article III standing and standing under the Tucker Act, which "imposes more stringent standing requirements than Article III." *Wks. Marine v. United States*, 575 F.3d 1352, 1359 (Fed. Cir. 2009).

The Tucker Act requires a plaintiff to show it is an interested party who was prejudiced by a significant error in the procurement process. *Associated Energy Grp., LLC v. United States*, 131 F.4th 1312, 1319 (Fed. Cir. 2025) (citing *Diaz v. United States*, 853 F.3d 1355, 1358–59 (Fed. Cir. 2017)). A plaintiff is an interested party if it (1) was an actual or prospective bidder

who (2) had a direct economic interest in the protest, meaning it had a substantial chance of winning the contract. *Id.* And a plaintiff establishes prejudice by demonstrating that but for the defendant's error, it would have had a substantial chance of securing the contract. *Id. See also REV, LLC v. United States*, 91 F.4th 1156, 1163 (Fed. Cir. 2024) (citations omitted). "Put another way, to show prejudice a disappointed bidder needs to show that 'it had greater than an insubstantial chance of securing the contract if successful on the merits of the bid protest.'" *REV, LLC*, 91 F.4th at 1163 (citation omitted). Prejudice must be shown either as a part of or in addition to a showing of direct economic interest. *Id.* (quoting *CliniComp Int'l, Inc. v. United States*, 904 F.3d 1353, 1358 (Fed. Cir. 2018)).

Under the Administrative Procedure Act standard, "a bid award may be set aside if either: (1) the procurement official's decision lacked a rational basis; or (2) the procurement procedure involved a violation of regulation or procedure." *Impresa Construzioni Geom. Domenico Garufi v. United States*, 238 F.3d 1324, 1332 (Fed. Cir. 2001) (citations omitted). When a challenge is brought under the former provision, a reviewing court must decide whether "the contracting agency provided a coherent and reasonable explanation of its exercise of discretion." *Id.* at 1333 (citation omitted); *Axiom Res. Mgmt., Inc. v. United States*, 564 F.3d 1374, 1381 (Fed. Cir. 2009) (citation omitted). And the deference afforded to the agency is even greater when the reviewing court assesses a technical evaluation. *HealthRev, LLC v. United States*, 172 Fed. Cl. 73, 85 (2024) (citing *Axiom Res. Mgmt.*, 564 F.3d at 1381). Further, the "disappointed bidder bears a heavy burden of showing that the award decision had no rational basis." *Impresa*, 238 F.3d at 1333 (quotation marks and citations omitted).

A plaintiff's mere disagreement with the contracting agency's judgment is insufficient to sustain a protest. *HealthRev*, 172 Fed. Cl. at 87 (citing *Banknote Corp. of Am., Inc. v. United States*, 56 Fed. Cl. 377, 384 (2003), *aff'd,* 365 F.3d 1345 (Fed. Cir. 2004)). "Evaluation of experience and past performance, by its very nature, is subjective[,] and an offeror's mere disagreement with an agency's evaluation judgments does not demonstrate that those judgments are unreasonable." *Gritter Francona, Inc. v. United States*, 158 Fed. Cl. 597, 608 (2022) (cleaned up) (quoting *Sci. & Mgmt. Res., Inc. v. United States*, 117 Fed. Cl. 54, 65–66 (2014)). "De minimis errors in the procurement process do not justify relief." *Sallyport Glob. Holdings, Inc. v. United States*, 129 Fed. Cl. 371, 378 (2016) (citation omitted).

Bidders "carry the burden of presenting an adequately written proposal, and an offeror's mere disagreement with the agency's judgment concerning the adequacy of the proposal is not sufficient to establish that the agency acted unreasonably." *Integrated Fin. & Acct. Sols., LLC v. United States*, 161 Fed. Cl. 475, 490 (2022) (quotation marks and citation omitted); *HealthRev*, 172 Fed. Cl. at 87 ("[T]he onus [is] on the [offeror] to submit a well-written proposal with adequately detailed information.") (some alteration in original) (quotation marks and citation omitted). And the contracting agency does not act arbitrarily by judging a proposal on its actual text. *Integrated Fin.*, 161 Fed. Cl. at 490 (citing *Asset Prot. & Sec. Servs., L.P. v. United States*, 5 F.4th 1361, 1366 (Fed. Cir. 2021)).

IV. Discussion

Plaintiff's Amended Complaint is based primarily on its contention that DHS incorrectly evaluated Ms. [***]'s resume, concluding she lacked four years of specialized experience involving continuous monitoring. It points out the Solicitation only required offerors to show their proposed key personnel met the minimum requirements in the RFQ. *See, e.g.*, Pl.'s Mot. at 11 (citation omitted). And the RFQ did not explicitly define continuous monitoring. Tab 15a at AR 735 ("Resumes must clearly demonstrate the proposed personnel meet the key personnel minimum qualifications."); Pl.'s Resp. at 3 (alleging Section 2.8.4, which lists continuous monitoring tasks under the RFQ, "provides the only reasonable basis for defining 'continuous monitoring' for the purposes of this RFQ"). A proffered Cybersecurity Reporting Lead only needed to exhibit "at least four years of specialized experience involving continuous monitoring." Pl.'s Mot. at 11 (quoting Tab 15a at AR 779). Plaintiff believes it was prejudiced because "DHS abandoned the terms of the RFQ and evaluated Saliense under a strict standard that was not in the Solicitation and was not applied to other offerors." *Id.* at 9. These purported errors led DHS to assign Saliense a deficiency, which rendered it ineligible for the award. *See, e.g.*, Pl.'s Mot. at 1–2.

Saliense also argues DHS "prejudicially and disparately transformed" the Solicitation's requirements for the Cybersecurity Reporting Lead through unstated evaluation criteria. Pl.'s Mot. at 10 (citation omitted); Pl.'s Reply at 1. First, it alleges Mr. Yeske's typographical error changed the Cybersecurity Reporting Lead to a position focused entirely on continuous monitoring. Pl.'s Mot. at 10. Second, Defendant purportedly distorted the requirement for the Lead to have experience *involving* continuous monitoring. *Id.* Instead, Saliense asserts Defendant mandated the Lead have at least four years of experience *in* continuous monitoring—which Saliense claims is a significant modification to the Solicitation's terms. Pl.'s Mot. at 15–16. Third, DHS impermissibly used a definition of continuous monitoring not included in the Solicitation. In addition, it improperly faulted Ms. [***]'s resume for failing to show experience in every task laid out in Sections 2.8.4 and 4.3.3 in the RFQ. Pl.'s Mot. at 11–12, 15. Finally, according to Plaintiff, DHS applied these purported unstated requirements only to Saliense's Cybersecurity Reporting Lead and not to Delviom's proposed Lead. *See* Pl.'s Mot. at 19.

As explained below, these arguments are unpersuasive. The Agency permissibly found fault with Ms. [***]'s experience in continuous monitoring. DHS' actions were not arbitrary or capricious or contrary to law, and it reasonably found Plaintiff's resume did not sufficiently demonstrate Ms. [***] had the four years of specialized experience in continuous monitoring as required by the Solicitation. Accordingly, since Defendant's decision meant Plaintiff was ineligible for the award, Saliense does not have statutory standing to proceed with the remainder of its claims.

A. Unstated Evaluation Criteria

A reviewing court must defer to an agency's technical assessment of an offer. *HealthRev*, 172 Fed. Cl. at 85 (citing *Axiom Res. Mgmt.*, 564 F.3d at 1381). As part of the "minutiae of the procurement process," contracting officials may make discretionary

determinations about the sufficiency of proposed key personnel's experience, which "a court will not second guess." *E.W. Bliss Co. v. United States*, 77 F.3d 445, 449 (Fed. Cir. 1996) (citations omitted). *See also Impresa*, 238 F.3d at 1332. Instead, a court must examine whether the procuring agency provided "a coherent and reasonable explanation of its exercise of discretion." *HealthRev*, 172 Fed. Cl. at 82, 85 (first quoting *Impresa*, 238 F.3d at 1333; and then quoting *Axiom Res. Mgmt.*, 564 F.3d at 1381).

"It is hornbook law that agencies must evaluate proposals and make awards based on the criteria stated in the solicitation." *Banknote Corp.*, 56 Fed. Cl. at 386. To succeed on a claim for unstated evaluation criteria, a plaintiff must show "(i) the procuring agency used a *significantly different basis* in evaluating the proposals than was disclosed; and (ii) the protester was prejudiced as a result—that it had a substantial chance to receive the contract award but for that error." *HealthRev*, 172 Fed. Cl. at 89 (emphasis added) (quoting *Banknote Corp.*, 56 Fed. Cl. at 387).

1. The Agency's Typographical Error Does Not Mean It Used Unstated Evaluation Criteria.

Saliense argues DHS transformed the Cybersecurity Reporting Lead into a position focused principally on continuous monitoring. Pl.'s Mot. at 10 (citing Tab 77 at AR 2425). Plaintiff explains "[e]ssentially, DHS took a single aspect of the Cybersecurity Reporting Lead's qualifications—the requirement to show 'four years of specialized experience *involving* continuous monitoring'—and made it into the *entire purpose* of the position." *Id.* To support its claim, Saliense points to Mr. Yeske's mistake in his memorandum to Ms. Buggs and a line in a letter it received notifying it of the results of the corrective action, which imprecisely summarized the requirements for the Cybersecurity Reporting Lead. *See* Pl.'s Mot. at 10 (citations omitted); Am. Compl. at 3, 11, 17 (citing Tab 78.2 at AR 2435 ("The Government requires four (4) years of specialized experience in Continuous Monitoring.")); Tab 77 at AR 2425 (citing Tab 15a at AR 779).

In two paragraphs summarizing the technical evaluation team's conclusions, Mr. Yeske incorrectly refers to the Cybersecurity Reporting Lead as the "Continuous Monitoring Lead" when he informs Ms. Buggs that Saliense's proposed candidate lacked the "require[d] four (4) years of specialized experience in Continuous Monitoring for this key position." Tab 77 at AR 2425. This is the only place in the record where Defendant refers to the Cybersecurity Reporting Lead as the Continuous Monitoring Lead. *See, e.g.*, Tab 76; Tab 77; Tab 36a (Delviom's Factor 3 Evaluation). Plaintiff asserts this was not "merely a typographical error." Pl.'s Reply at 2. Mr. Yeske's mistake "confirms that Saliense was subject to unstated evaluation requirements" because continuous monitoring only accounted for a portion of the experience and responsibilities of the Cybersecurity Reporting Lead. *Id.*

Defendant disagrees. It points out it was important for the Cybersecurity Reporting Lead to have experience in continuous monitoring and argues "[t]he reference in the corrective action decision to this position as the Continuous Monitoring Lead therefore simply reflected the actual responsibility of the position and nothing more." Def.'s Resp. at 2. It emphasizes "nothing in

the record shows that the Government applied a heightened bar of requiring Saliense's proposed personnel, Ms. [***], to have four years of experience in a 'job that was singularly dedicated to continuous monitoring.'" *Id.* at 2–3 (quoting Pl.'s Mot. at 10).

Delviom also contests Saliense's claims, arguing Mr. Yeske's "misstatement regarding the position title is nothing more than a non-prejudicial typographical error." Def.-Intervenor's Resp. at 11. "[T]he record reflects that the Agency determined Saliense to be ineligible due to the lack of *any* experience in continuous monitoring—not because the Agency held Saliense to a more rigorous standard than the RFQ required." *Id.* at 11–12. And, Defendant-Intervenor stresses, Mr. Yeske's mistake does not negate "the substance of the Agency's reconsideration memorandum nor the underlying evaluation of Saliense under Factor 3." *Id.* at 11; *see also* Def.-Intervenor's Reply at 4–5 (stating "the use of the term 'Continuous Monitoring Lead' is transparently a typographical error with no impact on the Agency's evaluation of Saliense's Cybersecurity Reporting Lead and the extent to which she had the required continuous monitoring experience").

While Mr. Yeske did incorrectly refer to the position at issue as a "Continuous Monitoring Lead," this error does not demonstrate the procuring officials transformed the Cybersecurity Reporting Lead into a job focused solely on continuous monitoring. "[S]mall errors made by the procuring agency are not sufficient grounds for rejecting an entire procurement." *Grumman Data Sys. Corp. v. Widnall*, 15 F.3d 1044, 1048 (Fed. Cir. 1994) (citation omitted). And overturning awards for de minimis errors is needlessly disruptive of government programs and procurements. *Id.* (citations omitted).

In fact, the record supports that this was likely a typographical error. Defendant repeatedly refers to the position under its correct title throughout its evaluation of Ms. [***]'s resume. *See, e.g.*, Tab 76 (reevaluating in detail the proposed Cybersecurity Reporting Lead's resume). Defendant found Ms. [***] demonstrated the required ten years of cybersecurity experience for the Cybersecurity Reporting Lead role. *Id.* at AR 2415. Its only objection to her resume stemmed from her failure to demonstrate the required four years of specialized experience involving continuous monitoring. *Id.* at AR 2413 ("[T]here is no evidence in the resume that this individual has served in a capacity where their professional responsibilities would have included active monitoring of systems to ensure continued compliance with cybersecurity requirements in operations."). DHS reviewed Ms. [***]'s resume role by role, bullet by bullet looking for said continuous monitoring experience. *Id*. at AR 2415–19.

Mr. Yeske's error was de minimis. And it does not lend credence to Saliense's assertion that Defendant transformed the Cybersecurity Reporting Lead into a Continuous Monitoring Lead.

2. DHS Used the Plain Meaning of Involving.

Saliense claims the Agency substituted "in" for "involving" in a critical provision of the Solicitation. Pl.'s Mot. at 10; Am. Compl. at 17–18. Plaintiff avers that rather than requiring the Cybersecurity Reporting Lead to have at least four years of specialized experience *involving*

continuous monitoring, Defendant evaluated Saliense's proposed candidate for four years of specialized experience *in* continuous monitoring. Pl.'s Mot. at 10. This argument is unavailing.

Plaintiff instructs that, as used here, "involving continuous monitoring" must mean "to meet the qualification criteria, a candidate would only need to demonstrate prior experience that included *some* continuous monitoring activities." *Id.* In contrast, "in continuous monitoring" refers to "a job that was singularly dedicated to continuous monitoring." *Id. See also* Am. Compl. at 17–18. Saliense again argues DHS transformed the RFQ's conditions to require the Cybersecurity Reporting Lead have four years of experience *exclusively* in continuous monitoring. Pl.'s Mot. at 10. And Plaintiff believes only its application was evaluated under this heightened standard. *Id.*

The language in a solicitation is not ambiguous simply because the parties differ in their respective interpretations of a term. *See NVT Tech., Inc. v. United States*, 370 F.3d 1153, 1159 (Fed. Cir. 2004) (citation omitted) (applying principles of contract interpretation to decipher solicitations in procurement cases). An RFQ, "like any contract, must be read in light of its purpose and consistently with common sense." *Stratos Mobile Networks USA, LLC v. United States*, 213 F.3d 1375, 1380 (Fed. Cir. 2000) (citation omitted).

Merriam-Webster's defines "involving" as "to relate closely," "to have within or as part of itself: include," or "to require as a necessary accompaniment: entail." Merriam-Webster's Collegiate Dictionary, 660 (11th ed. 2020). In comparison, "in" is "used as a function word to indicate limitation, qualification, or circumstance < alike ~ some respects >." *Id.* at 627. These words serve similar purposes in the context of the disputed sentence.

The language at issue here is not cryptic even if Saliense's reading of "involving" differs from the Agency's or Delviom's view. Defendant's interpretation of involving adhered to the plain meaning of the word. While it did inexactly explain it "require[d] four (4) years of specialized experience in Continuous Monitoring" in a letter to Saliense *after* it completed its evaluation, the Agency consistently used the correct standard throughout its actual evaluation of Plaintiff's proposal. Tab 78.2 at AR 2435. *See also* Tab 76. And its explanation of its evaluation of Ms. [***]'s resume acknowledged her ample experience involving cybersecurity—all of which it gleaned from her resume. *See* Tab 76 at AR 2413–19. Instead, the Agency explained, the resume did not demonstrate *any* experience that related closely to or included continuous monitoring. *Id.*; Tab 77 at AR 2425 ("The reevaluation affirmed the TET's original conclusion that the proposed resume failed to demonstrate any experience in Continuous Monitoring."). Its evaluation criteria did not differ from what was disclosed in the RFQ.

3. Defendant Applied a Reasonable Definition of Continuous Monitoring.

Saliense next asserts the Agency impermissibly used an unstated definition of continuous monitoring. It points to references to NIST SP 800-137 and NIST RMF in the evaluation, arguing DHS unfairly relied on the definition of continuous monitoring in these documents to redefine the term in the RFQ. Am. Compl. at 18–19; Pl.'s Resp. at 3; Pl.'s Mot. at 15–16. Even as it argues that "Section 2.8.4 provides the only reasonable basis for defining continuous

monitoring for the purposes of this RFQ," Plaintiff contradicts itself and complains it was penalized for "failing to demonstrate experience performing *all* identified tasks in RFQ Sections 2.8.4 and 4.3.3." Pl.'s Resp. at 2–5 (quotation marks omitted). *See also* Pl.'s Mot. at 18–19.

In this case, the procurement officials refer repeatedly to the definition of continuous monitoring in NIST SP 800-137, as well as the requirements of Sections 2.8.4 and 4.3.3, which outline the tasks and responsibilities of the Cybersecurity Reporting Lead pertaining to continuous monitoring. *See generally* Tab 76. Plaintiff argues the RFQ did not specifically incorporate NIST SP 800-137. Pl.'s Resp. at 3. Instead, these documents were listed only to help the eventual awardee with their performance. *Id.*

At the same time, Saliense claims the Solicitation did not require a proposed Cybersecurity Reporting Lead's resume to demonstrate experience with every listed responsibility in Sections 2.8.4 and 4.3.3, even as it argued that those sections formed the only permissible basis to define continuous monitoring. Pl.'s Resp. at 3–4. *See also* Def.'s Reply at 3–4 (pointing out the inconsistencies in this argument with Plaintiff's preferred definition of continuous monitoring).

Defendant disagrees, claiming guidance documents like NIST SP 800-137 provided context which helped offerors and the Agency understand the continuous monitoring experience requirement. *See* Def.'s Mot. at 9. And it gives a contrasting interpretation of the role Sections 2.8.4 and 4.3.3 play in the Solicitation, arguing these sections simply "listed requirements relating to continuous monitoring within a particular sub-task." Def.'s Mot. at 10–12. *See also* Def.-Intervenor's Mot. at 11–12 (alteration in original) (quoting Tab 15a at AR 767–68) ("As is typical in a SOW, the Government outlined the work '[t]he Contractor shall' perform in several task areas."). To comply with the FAR, DHS was required to provide these "description[s] of work to be performed" in the Solicitation's SOW. FAR 8.405–2 (2024).

To interpret a solicitation, the reviewing court should begin with the language of the written agreement. *NVT*, 370 F.3d at 1159 (citation omitted). "[T]he document must be considered as a whole and interpreted so as to harmonize and give reasonable meaning to all of its parts." *Id.* (citation omitted). And "a solicitation need not identify each element to be considered by the agency during the course of the evaluation where such element is intrinsic to the stated factors." *Banknote Corp.*, 56 Fed. Cl. at 387 (citations omitted). To show ambiguity it is not enough that the parties differ in their respective interpretations of a contract term. *NVT*, 370 F.3d at 1159 (citation omitted).

The Solicitation does not support Saliense's position that the Agency could not rationally use the definition of continuous monitoring in NIST SP 800-137. As explained above, the RFQ explicitly instructed that the DHS Information Systems Continuous Monitoring strategy "must be complied with to meet the requirements" of the contract. Tab 15a at AR 742. And the guidance defined continuous monitoring using the definition in NIST SP 800-137. Tab 12f at AR 259. The RFQ also separately listed NIST SP 800-137 as an instrument that "may be helpful to the contractor in performing the tasks described in the document[]." Tab 15a at AR 743. The NIST interpretation of the term was intrinsic to understanding what specialized experience the

Cybersecurity Reporting Lead needed to demonstrate in her resume. Considering the Solicitation as a whole, it was reasonable for the Agency to rely on a definition of continuous monitoring within a document explicitly listed as helpful in the RFQ. *See NVT*, 370 F.3d at 1159.

Saliense's arguments about Sections 2.8.4 and 4.3.3 are similarly futile. *See, e.g.*, Pl.'s Resp. at 1–2. In Plaintiff's view, "the RFQ implicitly utilized Section 2.8.4 to define the types of relevant continuous monitoring that an offeror could use to meet the Factor 3 requirement." Pl.'s Reply at 3 (quotation marks omitted). It believes this is the straightforward reading of the RFQ. *Id.*; Am. Compl. at 8; Pl.'s Mot. at 11 (citing Tab 15a at AR 767–68); Pl.'s Resp. at 3.

Yet Saliense also objects to the Agency's reference to Sections 2.8.4 and 4.3.3 in its evaluation of the Offeror's proposal, arguing Ms. [***] did not need to demonstrate experience with every single duty in those sections. Pl.'s Mot. at 12–13. However, DHS noted Ms. [***]'s resume did not show familiarity with most of the responsibilities in Section 2.8.4 related to continuous monitoring and did "not fully cover all the required activities stated by the RFQ in section 4.3.3 for the Cybersecurity Reporting Lead role." Tab 76 at AR 2419. Ms. [***] "lack[ed] direct involvement in the more technical and developmental tasks, especially those related to continuous monitoring and tool development," and she was "missing governance, risk and compliance program tool development to support execution of continuous monitoring, staff performance management, quality of deliverables and risk quantification." *Id.*

Plaintiff has not met its heavy burden to establish DHS acted here without a rational basis. The Agency provided a "coherent and reasonable explanation of its exercise of discretion." *HealthRev*, 172 Fed. Cl. at 82, 85 (first quoting *Impresa*, 238 F.3d at 1333; and then quoting *Axiom Res. Mgmt.*, 564 F.3d at 1381). The record shows it thoroughly reviewed Ms. [***]'s resume in search of continuous monitoring experience and provided detailed and precise explanations for why each of her listed experiences did not constitute continuous monitoring. Tab 76 at AR 2415–19. Its reference to Sections 2.8.4 and 4.3.3 was merely part of that larger evaluation and cannot be divorced from its context.

There is no evidence DHS applied unstated evaluation criteria to Saliense's proposal. Thus, Saliense has not shown "the agency unreasonably downgraded its proposal for deficiencies that were substantively indistinguishable or nearly identical from those contained in other proposals." *Off. Design Grp. v. United States*, 951 F.3d 1366, 1372 (Fed. Cir. 2020) (quotation marks and citation omitted).

B. DHS Provided a Coherent and Reasonable Explanation of Its Exercise of Discretion.

Again, all of Saliense's arguments focus on the Agency's evaluation of Ms. [***]'s resume. Saliense quarrels with DHS' conclusion that Ms. [***] lacked the required experience in continuous monitoring. *See generally* Pl.'s Mot.; Tab 76; Tab 77. In its view, the agency discredits her proficiency in continuous monitoring as "mere assessment experience." Pl.'s Reply at 2 (quotation marks and citation omitted). Plaintiff argues descriptions like "[c]onducted systems risk assessment through risk analysis," "[r]esponsible for the development of security

control test plan and in-depth security assessment of information systems to maintain FISMA and FEDRAMP compliance," "[c]onducted I.T. controls risk assessment," and "provide advice on their adequacy, accuracy and compliance with FISMA and FEDRAMP" demonstrated she had experience involving continuous monitoring. Pl.'s Mot. at 16–17 (alteration in original) (citing Tab 33a at 1085–86). *See also* Pl.'s Resp. at 5–7. However, Defendant found these descriptions showed at most isolated post-assessment actions rather than ongoing continuous monitoring. Tab 76 at AR 2416.

Additionally, Saliense contends Defendant improperly penalized Ms. [***]'s resume because it did not use the exact words continuous monitoring. Pl.'s Mot. at 17 (citing *Guidehouse Inc.*, B-421227.2 et al., 2024 WL 4345107 (Comp. Gen. Aug. 26, 2024)). Plaintiff cites only to an unpersuasive and nonbinding GAO case to support this argument. In that case, the agency unreasonably relied on job titles alone—not on descriptions of experiences included on resumes—to determine a candidate was unqualified. *Guidehouse Inc.*, B-421227.2 et al., 2024 WL 4345107 (Comp. Gen. Aug. 26, 2024).

The Agency assessed Ms. [***]'s resume based on the actual text Saliense provided in its bid. Its actions were not arbitrary simply because it evaluated the resume on its face. *See Integrated Fin.*, 161 Fed. Cl. at 490 (citation omitted); *Trumble Constr. v. United States*, 172 Fed. Cl. 43, 53 (2024). And the Court cannot sustain a protest based solely on Saliense's disagreement with the Agency's reasonable decision. *See HealthRev*, 172 Fed. Cl. at 87 (citing *Banknote Corp.*, 56 Fed. Cl. at 384).

C. Saliense Lacks Statutory Standing for its Remaining Claims.

Delviom and DHS both argue that since Saliense could not receive the award, it does not have statutory standing for its additional claims. Def.'s Mot. at 12–13; Def.'s Resp. at 9; Def.-Intervenor's Mot. at 16–17. This is the basis of Delviom's Motion to Dismiss under Rule 12(b)(1) of the Rules of the Court of Federal Claims.

In procurement cases, statutory standing is not jurisdictional. *CACI, Inc.-Federal v. United States*, 67 F.4th 1145, 1151 (Fed. Cir. 2023) (citations omitted). When a plaintiff argues the reviewing agency incorrectly or impermissibly evaluated the bid of another contractor, the Court must determine whether the plaintiff is an interested party for purposes of statutory standing. *Id.* at 1152. To establish statutory standing for its remaining claims and demonstrate it is an interested party and sustained prejudice, Saliense must show at least a substantial chance it could have been the awardee under the Solicitation had it not been for the errors it believes infected the procurement process. *REV, LLC*, 91 F.4th at 1163.

Because Saliense's proposal has a disqualifying deficiency, it fails to show it is prejudiced under the standing analysis. "[P]rejudice analysis is concerned with the impact the alleged error in the procurement process has on the bidder's chances of succeeding." *Id.* at 1164 n.2. For the purposes of its prejudice analysis, the Court assumes if Saliense could proceed with its additional claims, it would prevail on the merits. *See id.*

Saliense cannot demonstrate there was a substantial chance it would have been the awardee if not for the purported errors that contaminated the procurement process. The Agency rationally found Plaintiff ineligible for the award based on its deficient Cybersecurity Reporting Lead. Since this deficiency made it ineligible for the award, Plaintiff lacks statutory standing for all its claims beyond those touching on Ms. [***]'s resume.

V. Conclusion

The Court **GRANTS** Defendant's and Defendant-Intervenor's Motions for Judgment on the Administrative Record, as well as Defendant-Intervenor's Partial Motion to Dismiss, ECF Nos. 24 & 26. It **DENIES** Plaintiff's Motion for Judgment on the Administrative Record, ECF No. 25. The Clerk is directed to enter Judgment.

IT IS SO ORDERED.

s/ Carolyn N. Lerner
CAROLYN N. LERNER
Judge